IoT 時代の情報セキュリティのあり方

ー今から始められる情報セキュリティ対策ー

アブストラクト

1. 背景

様々なモノがインターネットに接続されて、様々なシーンで活用される IoT（Internet of Things）時代が到来している。あらゆるモノがインターネットに接続されることで、ICT（Information and Communication Technology）を活用した我々の生活やサービスの利便性の向上をもたらすことが期待される。

一方、それに伴い新たな情報セキュリティリスクも発生しており、「IoT 機器の乗っ取り」や「標的型メール攻撃」「ランサムウェア」など、企業を取り巻くサイバー攻撃は高度化・巧妙化し続けている。このような状況下において、企業は情報セキュリティ対策の重要性を認識し、各社様々な形で対策を実施して、サイバー攻撃の脅威から自社や顧客を守ろうと努力している。

しかし、企業の努力とは裏腹に、サイバー攻撃による被害は増加傾向にある。この現状から、なぜ企業は情報セキュリティ対策を重要と考え対策を講じているにもかかわらず、サイバー攻撃による被害は減らないのかという疑問が浮かんできた。

本分科会では、情報セキュリティ対策の現状および情報セキュリティインシデントの発生原因を分析することで、現状の情報セキュリティ対策の問題点とその解決策を明らかにできると考え、その達成に向けて活動することとした。

2. 目的

本分科会では問題の解決に向け、特定の業種・業界によらず幅広く活用可能な「今から始められる情報セキュリティ対策」の成果を得ることを目的として活動する。情報セキュリティ対策の徹底を阻害している要因を明らかにし、その解決策を導き出すことで、本格的に到来する IoT 時代においても「安全安心」に ICT を利活用できるようにすることを目指す。

3. 問題解決に向けたアプローチ

本分科会では、情報セキュリティ対策の問題の究明および解決策を明らかにするために、以下の調査、研究を行った。

① サイバー攻撃の事例、動向に関する情報収集
② 情報セキュリティインシデントの調査・分析
③ サイバー攻撃に対する意識の調査・分析
④ 情報セキュリティ対策実施状況の調査・分析

上記の調査･分析した内容から問題を究明および解決するために、主に以下のアプローチを実施した。

（1） ロジックツリーを使用した原因分析

本分科会では、情報セキュリティインシデント事例の分析に対して、本フレームワークを用いて原因分析に向けたアプローチを行う。図 1 は IoT 機器の乗っ取り事例の分析例である。本原因分析では、「情報セキュリティポリシーが未策定」「サイバー攻撃に関する危機意識の欠如」「ICT/IoT の知識不足」の 3 点が原因として挙げられる。

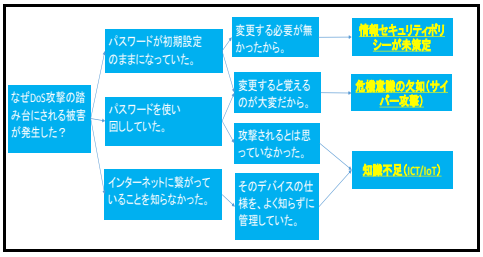

図 1 ロジックツリーを使用した分析例

（2）　ガイドラインを使用した問題解決

本分科会で作成した「IoT 時代のセキュリティ教育ガイドライン（以下、ガイドライン）」はサイバー攻撃から企業や顧客を守るために必要な情報が詰まった小冊子である。ICT/IoT を安全安心に利活用していく上で必要な情報として、ICT/IoT にはどのようなセキュリティリスクが存在し、どのような対策を講じるべきかを記述している。また情報セキュリティ教育の重要性や、情報セキュリティインシデント発生時に取るべき対応、運用方法などを記載している。

図 2 IoT 時代のセキュリティ教育ガイドライン（一部抜粋）

（3）　ツールを使用した可視化

本分科会で作成した「情報セキュリティ対策状況 可視化ツール（以下、可視化ツール）」は、自社の情報セキュリティ対策の実施状況を、対策の分類別に可視化することができるチェックリスト型のツールである。このツールを用いることで、自社の情報セキュリティ対策が不足している部分を明らかにし、必要な対策を講じることができるようになる。

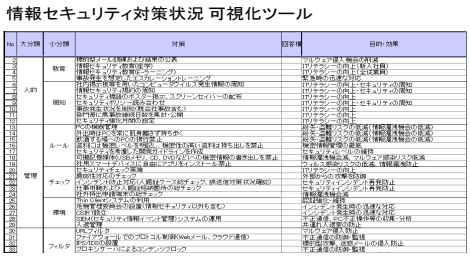

図 3 情報セキュリティ対策状況 可視化ツール（一部抜粋）

4. 成果

本分科会活動の結果、IoT 時代においても「基本的な情報セキュリティ対策を徹底」することが重要であることを改めて認識し、それを阻害している問題点を明らかにした。また、その問題解決策として「IoT 時代のセキュリティ教育ガイドライン」、「情報セキュリティ対策状況 可視化ツール」を作成し、以下の成果を挙げることができた。

- ICT/IoT の最新動向に関する情報提供による知識の底上げ
- サイバー攻撃に関する情報の周知による情報セキュリティ意識の向上
- 基本的な情報セキュリティ対策の実施意識率の向上
- 「今すぐ始められる情報セキュリティ対策」を実現するガイドラインおよびツールの開発

5. 総括

本分科会の研究成果は、IoT 時代に必要となる「今から始められる情報セキュリティ対策」を実現することができるものだと考える。ガイドラインは、IoT 時代にサイバー攻撃から身を守るために必要な情報セキュリティ対策のノウハウがまとめられており、この考え方を基に各社のスタイルに応じたカスタマイズを実施することで、より深化させることができる。また可視化ツールについては、自社の情報セキュリティ対策の実施状況を明らかにし、対策が不足している部分を浮き彫りにすることができる有用なツールである。

6. 提言

技術が進歩しても基本的な情報セキュリティ対策の徹底が重要であることに変わりはなく、IoT 時代こそ基本に立ち返り、自社の対策状況の把握や社員への周知・教育を行うことが最重要だと考える。そのために、まずは本分科会が作成した可視化ツールを活用し、自社の情報セキュリティ対策状況の実情を把握することから始めてみることを提言する。

以上